

*Received*  
FEB 13 1997

11 February 1997

In Reply Refer to:  
IEL-97-010

Department of Commerce  
Bureau of Export Administration  
Regulatory Policy Division  
Attn: Ms. Nancy Crowe, Room 2705  
14th Street and Pennsylvania Avenue, N. W.  
Washington, D. C. 20230

Dear Ms. Crowe:

Hughes Electronics Corporation provides the following comments on the Department of Commerce (DoC) Interim Rule on Encryption Exports. This Rule amends the Export Administration Regulations (EAR) to exercise jurisdiction over commercial encryption items. Hughes Electronics Corporation strongly supports the goal of enabling companies and their personnel to protect proprietary data and DoC regulated technical data being communicated overseas, but registers serious concerns about these regulatory changes and their implementation.

Our concerns fall into two broad categories:

- (1) Protection of proprietary information and technical data; and
- (2) Current and future global competitiveness and availability of American encryption products.

The globalization of our country's economy has led to increased cooperation with companies in foreign countries and the maintenance of offices in an ever increasing number of countries. This has challenged our ability to quickly and securely exchange information.

We believe that the implementation of the EAR Interim Rule will lead to the use of a weak encryption system, and/or the use of foreign-developed encryption systems. If the Interim Rule forces U.S. companies to use foreign encryption systems, we are at the mercy of the provider's government organization. According to the U. S. Government, the governments of some of the foreign providers are directing intelligence gathering efforts against U.S. Industry. Business reliance on foreign encryption systems could place U.S. data at risk.

Bureau of Export Administration  
IEL-97-010

11 February 1997

Page 2

84

One of our subsidiaries is a data communications service provider and must offer its customers communications privacy. We are dedicated to provide the best communications privacy technologically available from a cost-effectiveness stand-point.

A strong U.S. Government control approach will drive the body of encryption technical expertise to overseas locations, inaccessible to the U. S. Government. This does not seem the wisest strategy.

In the early 1990s, implementation of similar strong restrictive export controls was being examined relative to the evolving commercial computers and software. Today the U.S. is a major provider and exporter of computers and software as a result of export policies which induced U.S. industry to develop this technology in the U.S.

The burdens associated with registering distribution channels, and developing key escrow and key recovery mechanisms, will doom the domestic products, and enhance the development of similar products abroad.

Please recognize that our concerns, as expressed below, may not in all instances incorporate clear recommendations. We believe that any proposed changes should be based on follow-on coordination between DoC and industry.

Specific Concerns:

First, Key Escrow Recovery – this is an issue which needs serious review. Personal and corporate desires for information privacy, plus distrust of third party key escrow/recovery systems, promotes development of encryption systems without these features. We understand that U.S. Government policy and rulings favoring key escrow and key recovery have already stimulated the non-U.S. development and availability of alternative systems. These systems satisfy global consumer demands for strong cryptographic algorithms, and key sizes, but avoid the potential information compromise from the Key Escrow. Such systems have been announced and promoted at conferences in the U.S. since January 1997.

The restrictive U.S. policy on the export of strong encryption systems ignores the real loss of sales for U.S. developed encryption products and U.S. products incorporating encryption. The loss of sales quickly translates to the loss of manufacturing and distribution revenues including related employment. Shifting encryption manufacturing to non-U.S. sources fundamentally exports R&D, expertise, investments, potential developments, and improvements. It is ironic that the only controls available to the U.S. Government in such a scenario would be "Import controls", and that there would be no reasonable guarantee of privacy.

Bureau of Export Administration  
IEL-97-010

11 February 1997

Page 3 89

Second, The Key Escrow requirement is levied on the manufacturer of the encryption product with no notice or advice to the user. It appears that all U.S. suppliers have an ethical requirement to notify the consumer/end user, what weaknesses exist with the product. Additionally, the encryption item may already be installed in the system to be exported. Some manufacturers have indicated that they do not intend to enter into a "key escrow" arrangement. This poses problems for companies already domestically using a manufacturer's encryption product. Export of the same product to their foreign offices is prohibited. The provisions for the use of License Exception KMI do not provide any benefit, since they also require a commitment to the development of key recovery systems. Even when the manufacturer commits to a key escrow development, end users are at risk of not being able to support or use previously exported products if the manufacturer's Exception is not renewed.

Third, the responsibility of integrators of products that incorporate encryption technology is not clear. We request a clarification of the responsibilities of the integrators of products which incorporate encryption technology.

Fourth, the transition of responsibility for all non-military cryptographic products from the Department of State (DoS) to DoC permits the temporary export of portable computers for international business travel using License Exceptions TMP and BAG. Unfortunately, the temporary export of portable computers with installed non-military cryptographic software under the Exemption, "tools of trade", is limited to items owned by the individual. While we understand that the U.S. Customs' practice has been to allow company owned equipment and software to be treated as "tools of the trade owned by the individual", we can not encourage our travelers to ignore and violate the wording of the EAR. This "limit on eligibility" for the Exception needs to be changed to include company owned equipment used as "tools of the trade".

Fifth, neither the Supplementary Information on the ITAR Final Rule, or the EAR Interim Rule addresses the applicability of ITAR Part 124.15, "Arrangements for U. S. encryption (Category XIII(b)(1) distribution by manufacturers." The DoC should consider a mechanism similar to this "distribution arrangement" that does not require the advance identification of foreign parties. Under the above ITAR arrangement, a company was allowed to enter into a proposed "distribution arrangement" with the DoS; without initially identifying the distributor(s), and only needed to make semi-annual reports of sales or transfers to DoS, identifying the distributor, quantity, type of article, U.S. dollar value, and purchaser or recipient of the encryption article. The Interim DoC ruling does not provide for such an arrangement; rather, the exporter is required to identify the distributor, all foreign consignees, foreign intermediate consignees, and end users in advance of the export.

Bureau of Export Administration  
IEL-97-010

11 February 1997

Page 4 *gy*

Also, under the Interim DoC rules, the distribution of a company's mass market software of 56 bps or greater requires key escrow features that are too expensive and difficult to implement. Companies were better able to operate under the ITAR. For these companies, the DoC Interim Rule is more cumbersome and prohibitive than the International Traffic in Arms Regulations (ITAR) "distribution arrangement" and places American companies at a competitive disadvantage.

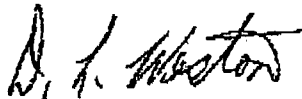
Sixth, HE recommends revision of the EAR Interim Rule, Part 742.15, Paragraph (4)(ii) to read:

"(ii) Applications for encryption items not authorized under an encryption licensing arrangement. Applications for the export and re-export of all other encryption items will be considered on a case-by-case basis." (add) This applies to all commercial encryption commodities and software greater than 56 bit key length DES or equivalent strength."

Should you have any questions regarding this matter, please contact Kathryn Greaney of our Hughes office, Arlington, Virginia; telephone (703) 284-4286.

Yours truly,

HUGHES ELECTRONICS CORPORATION



D. L. Weston  
Manager  
International Export Licensing